

CLAIMS

What is claimed is:

1. A method for establishing a secure connection to a server for a user of a client computer on a network utilizing a Secure Sockets Layer (SSL) system, said method comprising:

storing a plurality of keyfiles in a data storage accessible to a client computer, each of said keyfiles comprising a unique private cryptology key and a unique digital certificate;

storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening one of said keyfiles;

in response to receiving one of said passwords input from a user, opening one of said keyfiles associated with said one of said passwords; and

transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said user.

2. The method of claim 1, further comprising:

storing an authentication data for said user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said user; and

identifying said user for opening a keyfile according to said unique identifier.

1 3. The method of claim 1, further comprising:
2 authenticating an identity of said user through a process of hashing, said
3 process including the steps of:
4 hashing a message into a hashed message using a hash function;
5 encrypting said hashed message into an encrypted hashed message
6 using said private cryptology key; and
7 transmitting said hash function, said message and said encrypted
8 hashed message to said server.

1 4. The method of claim 1, further comprising prompting said user for a password
2 through a Graphical User Interface (GUI) in a display associated with said client
3 computer.

1 5. A client computer for establishing a secure connection to a server for a user of
2 the client computer on a network utilizing a Secure Sockets Layer (SSL) system, said
3 client computer comprising:

4 means for storing a plurality of keyfiles in a data storage accessible to a client
5 computer, each of said keyfiles comprising a unique private cryptology key and a
6 unique digital certificate;

7 means for storing a plurality of passwords in said data storage, each of said
8 passwords being associated with a respective keyfile, each of said passwords being
9 capable of opening one of said keyfiles;

10 means for in response to receiving one of said passwords input from a user,
11 opening one of said keyfiles associated with said one of said passwords; and

12 means for transmitting from said client computer to a server a digital
13 certificate from said open keyfile to enable said server to authenticate an identity of
14 said user.

1 6. The client computer of claim 5, further comprising:

2 means for storing an authentication data for said user in said data storage, said
3 authentication data comprising a unique identifier that corresponds to a password for
4 said user; and

5 means for identifying said user for opening a keyfile according to said unique
6 identifier.

1 7. The client computer of claim 5, further comprising:
2 means for authenticating the identity of said user through a process of hashing,
3 said means for authenticating the identity of said user through said process of hashing
4 including:
5 means for hashing a message into a hashed message using a hash
6 function;
7 means for encrypting said hashed message into an encrypted hashed
8 message using said private cryptology key; and
9 means for transmitting said hash function, said message and said
10 encrypted hashed message to said server.

1 8. The client computer of claim 5, further comprising means for prompting said
2 user for a password through a Graphical User Interface (GUI) in a display associated
3 with said client computer.

1 9. A computer program product residing on a computer usable medium for
2 establishing a secure connection to a server for a user of a client computer on a network
3 utilizing a Secure Sockets Layer (SSL) system, said computer program product
4 comprising:

5 program code means for storing a plurality of keyfiles in a data storage accessible
6 to a client computer, each of said keyfiles comprising a unique private cryptology key
7 and a unique digital certificate;

8 program code means for storing a plurality of passwords in said data storage, each
9 of said passwords being associated with a respective keyfile, each of said passwords
10 being capable of opening one of said keyfiles;

11 program code means for in response to receiving one of said passwords input
12 from a user, opening one of said keyfiles associated with said one of said passwords; and

13 program code means for transmitting from said client computer to a server a
14 digital certificate from said open keyfile to enable said server to authenticate an identity
15 of said user.

1 10. The computer program product of claim 9, further comprising:

2 program code means for storing an authentication data for said user in said data
3 storage, said authentication data comprising a unique identifier that corresponds to a
4 password for said user; and

5 program code means for identifying said user for opening a keyfile according to
6 said unique identifier.

1 11. The computer program product of claim 9, further comprising:
2 program code means for authenticating the identity of the user through a process
3 of hashing, said program code means including:
4 program code means for hashing a message into a hashed message using
5 a hash function;
6 program code means for encrypting said hashed message into an encrypted
7 hashed message using said private cryptology key; and
8 program code means for transmitting said hash function, said message and
9 said encrypted hashed message to said server.

1 12. The computer program product of claim 9, further comprising:
2 program code means for displaying a Graphical User Interface (GUI) in a display
3 associated with said client computer; and
4 program code means for prompting said user for a password through said GUI.